Printers are dangerous

Hernández, J.C., Sierra, J.M., Gonzalez-Tablas, A., Orfila, A.
{jcesar,sierra, aigonzal, adiaz}@inf.uc3m.es

Security Group
Computer Science Department
University Carlos III of Madrid
28911 Leganés
Madrid, Spain

Abstract - In the last years, a lot of new intelligent full-featured peripherals that assist information systems have appeared. Those peripherals, such as printers, copiers, PDA organizers, web cameras, etc. usually have a very friendly way of configuration and managing (via http, ftp or telnet servers) and everyday offer more networked services. Their computation, memory and networking capabilities have also increased in the last years. Nowadays, many of them are comparable to workstations and run over complete operating systems such as Linux or Solaris.

All those factors imply that these devices could represent a real threat for the security of information systems. This problem is even worse because most of those peripherals have been considered inoffensive and not many administrators are aware about their security risks.

The most representative example is printers, which have been traditionally considered totally harmless devices. At present time, this idea is difficult to defend because too many security incidents related with networked printers have risen in the last years. System and security administrators have traditionally focused their efforts in fortifying servers and hosts only, but it seems that this view is not enough for assuring security nowadays.

Introduction

The field of computer security is quite heterogeneous, since many very different circumstances could affect to the security level of an information system. Printers, being components of information systems, must also be taken into account: Their capabilities have improved considerably and their relevance to security has also increased, accordingly. Some printers even use a Sparc CPU that runs the Solaris operating system, while others have Linux's network stack implementations. This close similarity with classical computers allows these

0-7803-6636-0/01/$10.00 ©2001 IEEE

peripherals a complex functionality, which usually involves higher security risks.

There are numerous incident reports were the abuse of printers have eased or even played a mayor role in hacker's activities. There are incidents due to a deficient configuration of these devices (configuration of these peripherals are usually worse, because they are considered inoffensive), and also incidents provoked by an insecure design or a bad implementation of some service of the device (commonly the software implemented is not properly tested and buggy, has backdoors, or is simply too old).

Networked printers are quickly growing in number and complexity. They have evolved towards an easier configuration, which in many cases can be done via ftp, telnet and http for the sake of user-friendliness and maintenance. In most of the cases, the manufacturers of these printers share the false idea that security is not an issue at all. This converts the election of the particular telnet/http/ftp server into a search for the cheapest and smallest available (in many cases it is on the firmware). Obviously, these objectives are clearly opposed to security. That explains why security vulnerabilities long ago discovered and patched in hosts are usually found in networked printers: the software in this devices has not evolved accordingly, suffering from trivial and classical attacks not affordable in any other applications.

This extremely simple and untested software/firmware is only one of the reasons that explain this kind of problems. The other common manufacturer's philosophy is not to make the printers simple and lightweight because of the inherent (CPU, hard drive, etc.) limitations but to make them very close to a real host, adding a real operating system, a powerful CPU, a full network connection, etc. If this is the option chosen by the manufacturer, and more and more chose it, it is completely evident how dangerous could be not to take its security seriously.

Even though printers do not usually keep important or sensitive information, they can be used for interrupting the proper working of the information system. An attacker that gains access to a networked printer could be able of using its TCP/IP communications to perform several attacks. Since the printer is not a regular host, probes coming from a network printer might pass unobserved. These devices do not usually maintain detailed logs, which makes very difficult to trace back hacker's tracks.

Typical attacks

There are two kinds of attack in which a printer can be useful or needed: The first class of attacks happens when the intruder exploits security vulnerabilities

found in the printer itself (faulty software, badly configured services, etc.) and the second one happens when the intruder exploits some printer properties that are not specifically someone's mistake (networked printers are excellent *idle machines* in the night).

The first of these two types of attacks is, by far, the most frequent and easy to solve, because in most of the cases, after a vulnerability is reported, the manufacturer quickly distributes patches with a solution. The second one is more difficult to stop, but there are lots of things the security administrator can do to prevent it or to minimize its impact.

Into the next subsections we will show several examples of how printers can be used to develop hacker attacks. These subsections show how an attacker could gain root access into certain network printers, obtain other users login/password, interrupt the printer regular working and hide him/her tracks.

JETDIRECT vulnerabilities

The HP JetDirect is a famous device widely used in many organizations. In October 2000 multiple vulnerabilities were discovered, which if exploited by a hacker could make it inoperative. These vulnerabilities are caused by buffer handling problems in the firmware. Furthermore, another bug exits in the Jetdirect IP protocol implementation. This error can cause the printer to crash if a certain malformed packet is sent to the printer.

HP has produced a new firmware version that solves this problem, which can be downloaded from its web site. However, the vast majority of the administrators are not aware of those problems, which implies that there are many Jetdirects working with the old firmware version.

Buffer handling problems are serious menaces to security, but nowadays, although constantly appearing in diverse applications, are well known and easy to prevent. The discovery of various buffer handling problems in JetDirect's firmware reveals a serious lack of security consciousness during its development.

QMS 2060 vulnerability

This bug enables root access to the printer without any password protection. The access to the printer is guaranteed by a user/password file (passwd.ftp), only the users specified into this file can access to it. However if an attacker tries to login with the root login, s/he will access to the printer independently of the password typed.

The security implications of this bug cannot be bigger; the attacker could do what ever s/he wants with the printer (like obtaining the passwords of other

valid users, etc.) and also could perform attacks from the printer hiding all his/her tracks.

QMS customer support started an investigation for determining the grounds of the bug and they conclude that is was not a bug but a *feature*. In order to make the root password protected, one has to buy a "security key", a little DB-9 plug, which is plugged in the matching connector at the rear of the printer. Only then, a root password can be established (obviously, until then establishing a password file is totally meaningless).
This hard to believe bug is nowadays impossible to find in host's application, so here we have a clear example of how security was not a point at all in QMS's priorities.

Nashua Tec D445 vulnerabilities

The D445 Nashua Tec printer contains multiple vulnerabilities that make the printer open to several attacks:

1) It is possible to cause the crash of the authentication cgi, which is installed on the printer's HTTP configuration server. This makes also possible the execution of arbitrary code.

The password field (provided by the default logon page) is 15 characters long, but an intruder with a slightly modified copy of the original form will be able to submit many more characters (about 260 will be enough to crash) to the cgi and produce a buffer overflow. This could lead, after some work, to the execution of arbitrary code. Another unfortunate case of badly programmed cgi.

2) It is possible to use the printer for "ftp bounce attacks".

The ftp server does not check the type of port in the request (a port smaller than 1024 is an administrative port) nor checks the IP address used. So an intruder may use the ftp server to port scan some other hosts, anonymously abusing from the PORT ftp command. Obviously, no modern ftp server allows this ftp bounce attacks, so in this case we have met an old buggy software version.

3) It is possible to cause the printer to stop responding, effectively creating a Denial of Service attack by using an ICMP redirect storm against the printer communications stack.

Xerox's DocuColor 4 LP vulnerability

Xerox's DocuColor 4LP printer contains a vulnerability that allows remote attackers to cause the printer to stop responding and interrupt its regular working. The attack is based on a Denial of Service.

This attack is particularly easy to perform, because the attacker just needs to send a large amount of periods ('.') –around 2000 dots will be enough- in an HTTP request to the printer, a remote attacker can cause the printer to stop responding to pings and interrupt new and existing printing jobs. An attack that no serious web server can afford and which will take much time to correct until the administrators apply the patch.

HP 5M/5N vulnerability

This vulnerability allows an attacker to crash HP 5M or 5N printers just by sending a legitimate SNMP (Simple Network Managing Protocol) packet. The impact is not only that a person could crash only one printer, but rather that an attacker could severely impact printing in a fairly wide area.

Although Hewlett Packard has fixed the problem, this attack is still possible over many HP 5M/5N printers, and easy to perform after downloading the "npadmin" program from the ftp://pasta.penguincomputing.com/pub/prtools.

HP LaserJet 4M Plus DirectJet vulnerability

The LaserJet 4M Plus has an interesting security hole that allows anybody to sent a postscript document to print, even if the sender IP does not belong to the internal network. This printer keeps open the TCP ports 9099 and 9100 waiting for postscript documents to print. In [8] it is possible to find an *nmap* command for scanning networks to find printers with those ports open. When found, a simple tool like *netcat* will be more than enough to abuse this *feature*.

Although Hewlett Packard has fixed the problem, it is still easy to find those open ports waiting for huge postscript documents to print, interrupting other previously queued, and wasting paper resources.

Using printers to idlescan

After those examples we will see one technique that shows how attackers can use printers as *idle machines* for scanning other networks or machines without being traced and even causing, in some cases, legal problems to the security administrator of the network in which the printer is connected.

This interesting technique showed the dangers of predictable IP and ID packet numbering. Although any device with an IP and very low traffic is suitable for the use of this technique, printers are particularly adequate.

The idea is simple, but powerful: The scanning of the host can be conducted from the attacker's machine, using any IP spoofing tool to generate packets that have the idle printer IP as its origin address. The scan is performed by sending these forged packets to the real target while observing the idle printer. As the result of the scan will come back to the printer, it must be under constant observation to detect the arrival of an answer. This can be done with the aid of predictable IP numbering, just by continuously sending packets to it and observing the ID of the returning packet. When the scanned port is open, the scanned machine will return an answer to the printer, to which the printer will answer with an RST packet thus altering the answering pattern. This can be done twice for better accuracy. In this way, printers can be used to collect information previous to an attack in a very straightforward and reliable way. This method was presented and described in detail in [9], where the tool *hping* to perform this scan can be downloaded. This is another reason to take care and log all incoming and outgoing connections to an apparently harmless device.

Conclusions

Printers are not unique, in the sense that there are several intelligent peripherals and related software considered harmless with serious security vulnerabilities: for example, a vulnerability for the widely use Palm PDA which allows a Denial of Service attack over any computer running the Hotsync Manager Utility was discovered just months ago. Anyway, in this paper we have concentrated on networked printers since, at present, they mean the highest level of risk.

As we have shown, there should be no doubt about the security problem that networked printers represent. Apart from the previously seen vulnerabilities, it should be clear that many other security holes exist (from these and other manufactures) and have not been discovered yet. Printers are not inoffensive: networked printers must be taken into account as a very serious security risk, and thus must be updated and scanned regularly searching for vulnerabilities that could affect the proper working of the information system.

The best way of motivating manufacturers on improving the security of their products is customers demanding this security level. Administrators play an important role in this security improvement, because only if printers and the rest of devices are considered a potential risk, it will be possible that their security features get better.

References

[1] Securing your Network Printers from attacks
http://www.securiteam.com/securityreviews/Securing_your_Network_Printers_from_attacks.html

[2] IDLEScan, a stealth port scanner
http://www.securiteam.com/tools/IDELScan_-_a_stealth_port_scanner.html

[3] Securing your network printers from attacks
http://www.securiteam.com/sercurityreviews/3ASQIRFPPU.html

[4] The QMS 2060 security hole
http://archives.neohapsis.com/archives/bugtraq/1999-q3/0489.html

[5] HP series 5 printers denial of service
http://xforce.iss.net/static/1605.php

[6] The HP JetDirect J3111A buffer overflow in its internal web server.
http:// packetstorm.securify.com/9911-exploits/jetdirect.crash.txt

[7] HP JetDirect denial of service
http://www.infowar.com/iwftp/xforce/vol-3_num-3.html

[8] Hp LaserJet 4M Plus DirectJet Problem
http://lists.insecure.org/bugtraq/1997/Oct/0036.html

[9] New scanning method and the *hping* tool
http://www.kyuzz.org/antirez/software.html